121 Privacy of Information

Approved by President

Sidney A. McPhee, President

Effective Date: June 5, 2017, 2019

Responsible Division: President, Information Technology

Responsible Office: Information Technology, Office of the University Counsel

Responsible Officer: University Counsel, Vice President for Information Technology

I. Purpose

This policy establishes principles to guide the evolution of Middle Tennessee State University (MTSU or University) community standards of information privacy. This is a first step to clarify the level and protection of information privacy that may be expected by students/potential students, University employees, and outside persons on the campus community who have relationships with MTSU for whom MTSU collects information. This policy is intended to be flexible and independent of current definitions or concepts of technology and to rely, instead, on common sense and a culture supportive of mutual respect. While consideration has been given to the unique qualities of electronic information, this policy reflects the reasoning that the core value of privacy is not confined to any information medium.

While recognizing that other MTSU policies address other privacy issues, primarily those based on federal and state laws, the objectives of this policy are to ensure that:

A. A sharper focus is given to the University’s values and beliefs related to information privacy.

B. The expectations for maintaining information privacy are provided for University employees and students.

C. Information privacy guidelines are provided for University employees and students.

II. University Values and Beliefs

Where discretionary considerations are possible, a balanced approach to resolving conflicts between privacy and other values must incorporate the perspectives of the University as an institution, the collective behavior of employees and students, and the protection of individual privacy.
A. Institutional Perspective. MTSU must not be unduly constrained with respect to administrative efficiency in the enforcement of policies related to information privacy. Consideration should be given to the mission, internal control of information, and external mandates governing information collection and use. Each organizational unit to which privacy issues are of concern is encouraged to develop related procedures. Where practical, the decentralization of responsibility and the encouragement of employee participation in the development of relevant division or department operating procedures is the preferred method of increasing the level of learning and trust regarding information privacy issues.

B. Ethical Stewardship as a Collective Responsibility. Employees and students of MTSU are ethically obligated to respect the privacy of others and to adhere to a reasonable standard of conduct that supports this collective respect. For example, when employees gain unintentional access to information that a reasonable person would consider private, personal, or confidential, sensible actions are required, such as the notification of officials who are responsible for initiating corrective measures, or simply returning or forwarding the information to the intended recipient or owner.

C. The Individual’s Right to Know. While most employment related records are public, even confidential records can be accessed under certain conditions. Therefore, information in any form should be presumed capable of acquisition by others for purposes not related to the original creation of that information. In most instances, employees of MTSU have a right to know when their individual records have been reviewed, subpoenaed by parties external to MTSU, or are under review by MTSU officials or administrators who do not manage the information as part of their official duties. In such instances where it is administratively practical, the employees should be notified by email, phone call, or other means. Additionally, the Office of Human Resource Services (HRS) will maintain records of all requests for an employee’s public information. Records of requests for access are not made when the request is from University personnel as part of their job responsibilities. While most student related records are private, even confidential records can be accessed under certain conditions, such as through a judicial order or subpoena. In most instances, students will be notified of the compliance with a judicial order or subpoena by parties external to MTSU.

III. Student and Employee Records

A. Student Records. With regard to students’ education records, MTSU adheres to the federal Family Educational Rights and Privacy Act of 1974 (FERPA). Policy 500 Access to Education Records and FERPA provide students with the right to inspect and review education records, the right to seek to amend these records, and to limit disclosure of information from the records.
Therefore, the release of student information in any medium, including the internet, should be done only in accordance with FERPA and Policy 500 Access to Education Records.

1. Students have the right to restrict release of directory information as outlined in Policy 500 Access to Education Records.

2. Records are retained in accordance with Policy 129 Records Retention and Disposal of Records and the American Association of Collegiate Registrars and Admissions Officers (AACRAO) guidelines.

B. Employee and Faculty Records. HRS maintains the official personnel files for MTSU employees. Official faculty personnel files are maintained in the Office of the Provost. See Policy 811 Personnel Records. With the exception of records specifically deemed confidential by statute, all employee and faculty personnel information is public and accessibility is granted in compliance with Policy 120 Public Records – Inspecting and Copying.

IV. Web and Social Media Sites

MTSU respects the privacy of its students and employees and other constituents and is committed to ensuring that any personal or confidential information that is collected is kept accurate and secure from unauthorized access. MTSU may use third party analytics services that may use browser cookies to anonymously collect and track site usage information. This information is then analyzed as an aggregate and no personally identifiable information is collected.

A. Scope. This section applies to the University homepage and officially sponsored social media sites or groups, including http://www.mtsu.edu and any other official MTSU site. Since the MTSU web community consists of many websites, other websites may adopt more restrictive privacy and security statements as their specific needs require. The MTSU homepage, as well as other sites across campus, contain links to various external websites. The University is not responsible for the privacy and security practices or the content of external websites.

B. Information Gathered by MTSU.

1. Personal information provided via email or through other online means will be used only for purposes necessary to serve the needs of the person providing that information, such as responding to an inquiry or other request for information. This may involve redirecting the inquiry or comment to another person or department better suited to meeting the inquirer’s needs.
2. MTSU’s website does use server logs to collect information concerning users’ internet connection and general information about their visit to MTSU’s website. This information may be used to analyze trends, to create summary statistics for the purpose of determining technical design specifications, and to identify system performance or problem areas. This means the University sometimes acquires, records, and analyzes portions of the data that is entered into, stored on, and/or transmitted through this site by the user. This information is only released to the extent allowed or required by applicable law.

3. Such logging includes, but is not limited to:

   a. Hostname. The hostname and/or IP address of the user/client requesting access.
   b. System date. The date and time of the user/client request.
   c. Full request. The exact request the user/client made.
   d. Status. The status code the server returned to the user/client.
   e. Content length. The content length, in bytes, of the document sent to the user/client.
   f. Method. The request method used.
   g. Universal Resource Identifier (URI). The location of a resource on the server.
   h. Query string of the URI. Anything after the question mark in a URI.
   i. Protocol. The transport protocol and version used.
   j. E-mail address. In some cases, the e-mail address of the intended recipient of an e-mail may be logged when a link is accessed inside of an e-mail.

C. Cookies. A cookie file contains unique information that a website can use to track such things as passwords, pages the users have visited, the date the user last looked at a specific page, and to identify the user’s session at a particular website. MTSU does not use cookies to collect any information that could personally identify individual visitors.

D. E-Commerce. Some MTSU web sites may enable you to payment for products or services online with a credit card or other electronic payment mechanism. Unless otherwise noted, these transactions are encrypted. It is MTSU’s practice that confidential financial information will be used only for the purposes described in that transaction unless an additional use is specifically stated on that site. Data provided
specifically to facilitate credit card or other electronic business transactions are retained only for a reasonable time to effect the transaction.

E. Access to Information. Information collected from any MTSU website or social media group, including summary server log information, emails sent to the website or group, and information collected from web-based forms, may be subject to state and federal laws. This means that while MTSU does not actively share information, in some cases it may be compelled by law to release information gathered from its web servers or social media groups.

F. Information Usage. In the course of using the websites or social media groups, users may choose to provide information to the University via web forms, e-mail, or other electronic means. Personally identifiable information submitted will be used only for MTSU-related purposes. MTSU will not sell this data to outside parties. Requests for information and information submitted via forms on websites or social media groups will be directed to the appropriate staff to respond to those requests and may be recorded to help MTSU improve its site to better respond to similar requests. MTSU may use this information in any investigation of a potential violation of MTSU policies and procedures or as required by federal, state, or local law.

G. Security. Extensive security measures have been employed to protect against unauthorized access, disclosure, modification, or destruction of information under our the institution’s control, as well as the loss, misuse, or alteration of University websites, social media sites, and/or associated electronic information resources.

H. Contractors/Outsourced Development. Any entity contracted to develop or provide web or social media services is bound by and must follow this policy and Policy 920 Information Security, as well as all applicable University policies, in order to protect personally identifiable information (PII).

I. Web Analytics. Some MTSU websites use a third-party web analytics service to collect information such as URLs, internet domain and host names, browser software, and the date and time that the site is visited. This information is used to monitor the effectiveness of the website and to consider potential improvements to the website. The information is non-personal and is transmitted to and stored by the third party on its servers. MTSU does not share any specific information about a particular user. More information on web analytics is available by contacting the Information Technology Division.

V. Additional Privacy-Related Policies

Several current MTSU policies are directly or indirectly related to information privacy issues, illustrating the nature and complexity of the topic. These include the following:
A. Policy 150 Social Networking and Media

B. Policy 211 Misconduct in Scholarly Activities and Research

C. Policy 402 Protection of Human Subjects in Research

D. Policy 910 Information Technology Resources

E. Policy 920 Information Security

VI. Disciplinary Actions

Employees or students who access files or browse data of others, or access any information technology resources without authorization, for personal gratification or who engage in the unauthorized dissemination of information obtained from these resources, may have violated the privacy of others. If so, such behaviors are subject to disciplinary actions that are in proportion to the nature of the offense pursuant to institutional policy. Policy 851 Disciplinary Policy for Administrative and Classified Personnel and Policy 204 Tenure prescribe disciplinary actions and processes. In cases where employees dispute a charge, they may respond based on Policies 852 Administrative, Professional and Faculty Grievance or Complaint or 206 Tenure and Promotion Appeals Process. Refer to Policy 540 Student Conduct for disciplinary actions regarding students.

Forms: none.

Revisions: June 5, 2017 (original); ________, 2019 none.

Last Reviewed: June 2017 __________, 2019.

References: Family Educational Rights and Privacy Act of 1974; American Association of Collegiate Registrars and Admissions Officers Guidelines; Policies 120 Public Records – Inspecting and Copying; 129 Records Retention and Disposal of Records; 150 Social Networking and Media; 204 Tenure; 206 Tenure and Promotion Appeals Process; 211 Misconduct in Scholarly Activities and Research; 402 Protection of Human Subjects in Research; 500 Access to Education Records; 540 Student Conduct; 811 Personnel Records; 851 Disciplinary Policy for Administrative and Classified Personnel; 852 Administrative, Professional and Faculty Grievance or Complaint; 910 Information Technology Resources; 920 Information Security.